APPROVED: **DATE:**

Procedure No. 5-05
RISK ASSESSMENT

Purpose

A. To identify the threats facing the program or contract under audit and identify the controls or procedures the City has in place to prevent, eliminate, or minimize the threats.

B. To determine the probability that noncompliance and abuse, which is individually or in the aggregate material, could occur and not be prevented or detected in a timely manner by the internal controls in place and assess the internal control structure in accordance with SAS 55.

C. To develop audit procedures to see if the controls or procedures the City has in place to prevent, eliminate, or minimize identified threats are working and determine whether additional audit procedures are necessary to document threats actually occurring.

D. To document the audit program and results pertaining to the Risk Assessment phase of the audit.

Background

The rationale for conducting a Risk Assessment is that auditors can limit testing and focus on those areas most vulnerable to noncompliance and abuse. The extent of audit testing is directly related to an assessment of the activity's degree of vulnerability. The higher the vulnerability, the more extensive the audit testing needs to be and vice versa. Thus, even though an activity may have a high degree of inherent risk, a strong system of internal controls can reduce the entity's exposure to a low or moderate level. Accordingly, the need to conduct detailed audit tests could be reduced to an appropriate level. This produces a more cost-effective and timely audit.

1. Abuse – Abuse is distinguished from noncompliance in that abusive conditions may not directly violate laws, regulations, contracts, administrative procedures, or operating standards. Abusive activities may be within the letter of the laws, regulations, contracts, administrative procedures, or operating standards but violate either their spirit or the more general standards of impartial and ethical behavior.
2. Threat – A threat is an unwanted event or occurrence. It usually involves noncompliance or abuse of a law, regulation, contract, administrative procedure, or operating standard.
3. NIS - (Number of Items Susceptible) The number of the items (i.e., transactions, events, clerical operations, etc.) susceptible to the occurrence of the threat per year.
4. OR – (Occurrence Rate) The maximum threat occurrence rate or probability that a threat might occur on a susceptible item absent any internal controls.
5. ADM – (Average Damage Magnitude) The dollar value likely to be at stake in the event of a typical occurrence of the threat.
6. Initial Risk – The quantification (in terms of the actual cash lost or not collected or the cash outlays required to repair damages, pay for operating inefficiencies, or replace assets lost) of the losses due to the occurrence of an unwanted event (threat). Initial risk is computed using the formula: Initial Risk = NIS x OR x ADM.
7. Inherent Risk – The probability (high, moderate, or low) that a law, regulation, contract, administrative procedure, or operating standard related to audit objectives will be abused

or not complied with. This probability is determined with the use of the Vulnerability Assessment Guide – Threat Rating Table.

8. Vulnerability – The probability that noncompliance and abuse, which is individually or in the aggregate material, could occur and not be prevented or detected in a timely manner by the internal controls in place.

The audit team is allowed three work weeks to conduct the risk assessment, hold a risk assessment conference with the City Auditor, and develop audit procedures. If additional hours are required, the In-Charge Auditor should prepare a memorandum to the City Auditor describing the remaining work, reasons for the additional time and the additional time required.

Section 1 Procedure AUDIT FIELDWORK – PHASE I (RISK ASSESSMENT) Milestone #M-15

Purpose

To document the audit program and results pertaining to the Risk Assessment phase of the audit.

Background

The objectives of Risk Assessment are:

1. To identify the threats (unwanted events or occurrences) facing the program or contract under audit;
2. To identify the controls or procedures the city has in place to prevent, eliminate or minimize the threats;
3. To determine the probability that non-compliance and abuse, which individually or in the aggregate material, could occur and not be prevented or detected in a timely manner by the internal controls in place;
4. To assess the internal control structure (the control environment, control procedures, and the accounting systems) in accordance with SAS 55;
5. To develop audit procedures to see if the controls or procedures the city has in place to prevent, eliminate, or minimize identified threats are working; and
6. To determine if additional audit procedures are necessary to document threats actually occurring.

Procedure

Audit Staff	1. Obtain a copy of the City Auditor's Risk Assessment Audit Program and Results (APR) from Procedure No. 5-05A. 2. Modify the APR as necessary to accommodate the needs of the current audit assignment.
Supervising Auditor and City Auditor	3. Review and approve the Risk Assessment APR.
Audit Staff	4. File the Risk Assessment APR in the audit workpapers. 5. As the audit progresses, update the APR

Section 2 Procedure PREPARE LIST OF THREATS (Milestone #M-12)

Purpose

To identify the threats facing the program or contract under audit.

Background

A threat is an unwanted event or occurrence. It usually involves noncompliance or abuse of a law, regulation, contract, administrative procedure, or operating standard.

Procedure

Audit Staff	1. Based on information gathered during the Preliminary Survey, prepare a list of threats for the major audit areas identified during Mission Analysis. If computer-processed data are important or integral to the audit and the reliability of the data is crucial to accomplishing the audit objectives, include in the threats list the threats to the auditee's computer-processed data. 2. Submit the List of Threats to the Supervising Auditor and the City Auditor.
Supervising Auditor and City Auditor	3. Review and approve the List of Threats.
Audit Staff	4. File the List of Threats in the audit workpapers.

Section 3 AUDITEE'S DESCRIPTION OF INTERNAL CONTROLS TO ADDRESS THREATS LIST (Milestone #M-13)

Purpose

To identify the controls or procedures the auditee has in place to prevent, eliminate or minimize the threats.

Background

Internal controls are the combination of management objectives (policies) and techniques (procedures) used by managers to help ensure that their agencies, programs, or functions are effectively and efficiently managed in conformity with applicable laws and regulations.

Control objectives are the positive things agency managers want to happen or negative things they want to prevent from happening. Control objectives address the risks inherent in the work being done.

Control techniques are the procedures managers use to provide reasonable assurance that their control objectives are achieved—that is, to accomplish the positive things and prevent the negative things from happening.

Procedure

Audit Staff	1. Prepare cover letter for the List of Threats. 2. Send cover letter and List of Threats to the auditee.
Auditee management	3. Add any threats that are missing from the list. 4. Identify the Actual controls to mitigate those threats. 5. Provide the audit staff copies of written procedures describing the identified controls. 6. Return the List of Threats and Controls to the audit staff.
Audit Staff	7. File List of Threats and Controls in the audit workpapers.

Section 4: RISK MATRIX (Milestone #M-14)

Purpose

To summarize in a table the threats and controls pertinent to the audit subject.

Background

The Risk Matrix shows the relationship of threats and controls by identifying the specific controls that mitigate specific threats.

The Risk Matrix also classifies the controls as Actual or Potential. The controls marked "A" are Actual controls, as identified by the auditee. The controls marked "P" are Potential controls, as identified by the auditor based on his or her work during the preliminary survey. The potential controls may result in audit recommendations, depending on the outcome of subsequent controls testing and verification.

Procedure

Audit Staff	1. Prepare a Risk Matrix showing the controls that mitigate each threat (See Procedure No. 5-05E). 2. Initiate a finding development sheet (see Procedure No. M-22) for each potential control. 3. Submit the Risk Matrix and the finding development sheets to the Supervising Auditor and the City Auditor.
Supervising Auditor and City Auditor	4. Review and approve the Risk Matrix and the finding development sheets.
Audit Staff	5. File the Risk Matrix and the finding development sheets in the audit workpapers.